Claims

[c1] What is claimed is:

A system of protecting products against counterfeiting compromising the steps:

a) encoding a sequence by using a computer system;

b) method to assure that only unique sequences are calculated;

c) delivering the said sequence with a product;

d) transmit said sequence to a computer system;

e) verify said sequence by using a computer system to identify the consistency of said sequence;

f) verify said sequence with data stored on a said computer system to determine a product as original or as falsification;

g) report the result of verification.

[c2] A computer system of claim 1 to:

a) encode sequences and;

b) decode sequences and;

c) carry out tests of the consistency of encoded sequences and;

d) carry out comparison of said sequences with stored data on said computer system and;

e) store data on said computer system and;
f) legitimize parties to access the said computer system and;
g) legitimize parties to process data on the said computer system and;
h) generate and send messages.

[c3] A method of claim 1 of calculating the said encoded sequence by utilizing:
a) a symmetric encryption method or;
b) an asymmetric encryption method or;
c) by utilizing in addition a hash method to a symmetric encryption method or;
d) by utilizing in addition a hash method to an asymmetric encryption method.

[c4] Mthod sof claim 1 to assure that only unique encoded sequences arecalculated.

[c5] A method to control manufacturer for producing the same number of products as ordered by a customer by using encoded sequences and deliver the same number of encoded sequences to a manufacturer as number of products are ordered by a customer.

[c6] A method of protecting products against counterfeiting by delivering an encoded sequence with each piece of

product whereby the sequence:

a) is printed in readable form on the product or;

b) is engraved in readable form on the product or;

c) is printed as barcode on the product or;

d) is printed in readable form at the package of the product or;

e) is printed in readable form on a label that can be affixed to the product or the package of the product or;

f) is printed in readable form on a leaflet that is delivered with the product or;

g) is engraved as barcode on the product or;

h) is printed as barcode on the package of the product or;

i) is printed as barcode on a label that can be affixed to the product or the package of the product or;

j) is printed as barcode on a leaflet, which is delivered with the product or;

k) Is stored on a magnetic stripe that is delivered with the product or;

l) is stored on a radio frequency identification (RFID) tag that is delivered with the product or;

m) is stored on a the read only memory chip (ROM) in addition to the user data or;

n) is stored on a chip that is built in a product or;

o) is stored on any kind of digital data media or;

p) is stored on a compact disc-read (CD) or;

q) is stored on a digital versatile disc (DVD) or;

[c7] A method of proofing the authenticity of products by verifying the consistency of encoded sequences according claim 3 which are delivered with each piece of product by carrying out:
a) a symmetric encryption method;
b) a symmetric decryption method;
c) an asymmetric encryption method;
d) an asymmetric decryption method;
e) a symmetric encryption method and a hash method;
f) a symmetric decryption method and a hash method;
g) an asymmetric encryption method and a hash method;
h) an asymmetric decryption method and a hash method.

[c8] A method of determining products as original or as falsification by utilizing comparisons with data stored in files on computer systems according claim 2 when performing a proof of authenticity.

[c9] A method of determining the current place where a proof of authenticity of a product is carried out by using encoded sequences and computer systems according claim 2 and data stored in log files on computer systems according claim 2.

[c10] A method of tracing the chain of distribution of products

by using encoded sequences and computer systems according claim 2 and data stored in log files on computer systems according claim 2 when performing proofs of authenticity.